

Inhaltsverzeichnis

Abkürzungsverzeichnis	17
Einführung	23
Teil 1: Begriffe und Untersuchungsgegenstand	27
Kapitel 1: Der Spionagebegriff im Völkerrecht	27
A. Begriffliche Anhaltspunkte im humanitären Völkerrecht	28
I. Haager Landkriegsordnung	28
II. Protokoll I zu den Genfer Abkommen	28
B. Übertragbarkeit auf Friedensspionage	29
C. Krieg und Frieden; Arbeitsdefinition der Friedensspionage	30
I. Ermittlung fremder Geheimnisse	31
II. Staatliche und private Spionage	33
III. Spionageadressat	33
1. Spionage gegen Staaten	34
2. Spionage gegen Individuen	34
IV. Ort der Spionagehandlung	35
V. Heimlichkeit	35
VI. Definition der Friedensspionage	36
Kapitel 2: Erscheinungsformen der Spionage; Abgrenzungen	36
A. Spezialisierung	36
B. Prozessschritte	37
C. Fernerkundung und Aufklärung	38
D. <i>Intelligence</i>	39
Kapitel 3: Cyber und begriffliche Ableitungen	42
Kapitel 4: Untersuchungsgegenstand Cyberspionage im Völkerrecht	43
Teil 2: Technische Rahmenbedingungen und Bezugsfälle; Fallgruppen	45
Kapitel 1: Entwicklungsgeschichte und technische Grundlagen	45

Kapitel 2: Völkerrechtliche Relevanz durch Vernetzung	46
Kapitel 3: Bezugsfälle, insbesondere Vorgehensweise der UKUSA-Staaten	47
Unterkapitel 1: UKUSA-Vereinbarung/ <i>Five Eyes</i>	48
Unterkapitel 2: ECHELON-Abhörsystem	50
Unterkapitel 3: Horchposten in diplomatischen Vertretungen	51
Unterkapitel 4: SIGINT-Strategien der UKUSA-Staaten	52
A. Überwachung von Datenströmen	54
B. Zugriff auf Datenbestände	58
Kapitel 4: Fallgruppen	62
A. Einteilung nach Spionageadressaten	62
I. Staat-Staat	62
II. Staat-Privatakteur	63
B. Einteilung nach Spionageorten	63
I. Handlungs- und Erfolgsort auf eigenem Hoheitsgebiet (Inlandsspionage)	63
II. Handlungs- und Erfolgsort auf fremdem Hoheitsgebiet (Auslandsspionage)	63
III. Auseinanderfallen von Handlungs- und Erfolgsort (Divergenz)	64
Teil 3: Cyberspionage in zwischenstaatlichen Rechtsbeziehungen	65
Kapitel 1: Methodik der Untersuchung	65
Kapitel 2: Humanitäres Völkerrecht	68
Kapitel 3: Völkerrechtliche Verträge zur Friedensspionage; No spy-Abkommen	75
Kapitel 4: Friedensvölkerrecht und staatliche Herrschaftsbereiche	77
Unterkapitel 1: Allgemeines Gewaltverbot	78
A. Gewaltanwendung durch Cyberspionage	79
B. Cyberspionage zur Vorbereitung von Gewalthandlungen	81
Unterkapitel 2: Souveräne Staatengleichheit und Interventionsverbot	83
A. Verbotene Intervention durch Cyberspionage	85
I. Ausschließliche Zuständigkeit	86

II. Verbotener Zwang	88
B. Cyberspionage zur Vorbereitung verbotener Interventionen (sog. <i>Covert actions</i>)	92
C. Eingriffe in staatliche Gebietshoheit	93
I. Unbefugtes Eindringen in fremdes Hoheitsgebiet	94
1. Hoheitsfreie Räume	95
2. Einreise auf dem Luftweg	96
3. Einreise auf dem Seeweg	98
4. Einreise auf dem Landweg	99
II. Angemaßte Hoheitsgewalt	100
1. Hoheitliches Handeln	101
2. Innerstaatliche Hoheitsakte mit extraterritorialer Wirkung	102
3. Verbot hoheitlichen Handelns auf fremdem Hoheitsgebiet	106
4. Gewohnheitsrechtliche Ausnahme	111
a) Erklärungsdefizite der herrschenden Lehre	111
b) Gewohnheitsrechtliche Einschränkung staatlicher Souveränität?	114
Kapitel 5: Recht zwischenstaatlicher Organisationen	121
Unterkapitel 1: Vorrechte und Immunitäten der Vereinten Nationen	121
A. Unverletzlichkeit von UN-Räumlichkeiten	121
B. Unverletzlichkeit von UN-Kommunikation	125
C. Weisungsfreiheit von UN-Bediensteten	128
D. UN-Sonderorganisationen	130
Unterkapitel 2: Organisation der Parteien des Nordatlantikvertrags (NATO)	132
Unterkapitel 3: Sonstige zwischenstaatliche Organisationen	133
Kapitel 6: Recht der diplomatischen und konsularischen Beziehungen	135
A. Recht der diplomatischen Beziehungen	135
I. Cyberspionage des Entsendestaates	135
II. Cyberspionage des Empfangsstaates	137
B. Recht der konsularischen Beziehungen	138
Kapitel 7: Rechtfertigung von Cyberspionage	139
A. Vorherige Zustimmung	140

B. Notstand	140
Kapitel 8: Rechtswidrigkeitsfolgen und zulässige Gegenmaßnahmen	141
A. Rechtsfolgen	141
I. Recht der diplomatischen und konsularischen Beziehungen	142
II. Recht der Staatenverantwortlichkeit	144
1. Anspruch auf Einstellung und Unterlassung	144
2. Anspruch auf Wiedergutmachung	144
III. Recht der Vereinten Nationen	145
B. Völkerrechtlich zulässige Gegenmaßnahmen	146
I. Retorsion	147
II. Repressalie	147
C. Internationale Gerichtsbarkeit	149
Teil 4: Cyberspionage und Menschenrechtsschutz	151
Kapitel 1: Methodik der Untersuchung; Konventionsorgane	153
Kapitel 2: Anwendungsbereich von Konventionsrechten	156
Unterkapitel 1: Zeitlicher, persönlicher und sachlicher Anwendungsbereich	156
A. Zeitlicher Anwendungsbereich	156
B. Persönlicher Anwendungsbereich	157
C. Sachlicher Anwendungsbereich	158
Unterkapitel 2: „Räumlicher“ Anwendungsbereich; Jurisdiktionsklauseln	159
A. Territoriale Anwendung von Konventionsrechten	160
B. Extraterritoriale Anwendung von Konventionsrechten	161
I. EMRK	162
II. IPbpR	165
C. Übertragbarkeit auf Cyberspionage	168
I. Konventionaler Rechtsraum	169
II. Effektive Kontrolle fremder Gebiete	170
III. Herrschaftsgewalt und Kontrolle staatlicher Akteure	171
1. Handlungen diplomatischen und konsularischen Personals	172

2. Handlungen auf registrierten Schiffen und Flugzeugen	174
3. Auslieferung und Abschiebung	175
4. Einzelmaßnahmen gegen Personen	177
5. Virtuell ausgeübte Herrschaftsgewalt und Kontrolle?	178
a) EMRK	178
b) IPbpR	185
IV. Fazit	189
Kapitel 3: Verletzung von Konventionsrechten	190
Unterkapitel 1: Recht auf Achtung der Privatsphäre	190
A. Schutzbereich	190
I. Privatleben	191
II. Familienleben; Ehre und Ruf	192
III. Wohnung	194
IV. Korrespondenz und Datenschutz	195
B. Beeinträchtigung	198
I. Beeinträchtigung in Art. 8 Abs. 1 EMRK	198
1. Massenüberwachung	201
2. Individualüberwachung	203
3. Datenaustausch mit fremden Nachrichtendiensten	204
II. Beeinträchtigung in Art. 17 Abs. 1 IPbpR	206
C. Rechtfertigung	207
I. Schrankensystematik der Konventionen	207
II. Vereinbarkeit mit Art. 8 Abs. 1 EMRK	209
1. Gesetzesgrundlage	209
a) Bestehen einer innerstaatlichen Gesetzesgrundlage	209
b) Qualität der Gesetzesgrundlage	210
2. Legitimer Zweck	213
3. Notwendigkeit in einer demokratischen Gesellschaft	215
4. Die modifizierten Weber-Garantien	216
a) Gründe der Massenüberwachung (1)	216
b) Umstände individueller Kommunikationsüberwachung (2)	217

c) Genehmigungsverfahren (3)	219
d) Auswahl, Auswertung und Verwendung abgeschöpfter Daten (4)	221
e) Datenübermittlung an Behörden fremder Staaten (5)	222
f) Maßnahmendauer; Aufbewahrung und Vernichtung von Daten (6)	224
g) Interne Rechtsaufsicht (7)	225
h) <i>Ex post facto</i> -Kontrolle (8)	226
5. Rechtliche Garantien bei Individualüberwachung	227
6. Anwendungsfragen	231
7. Fazit	234
III. Vereinbarkeit mit Art. 17 Abs. 1 IPbpr	238
D. Schutzpflichten	243
Unterkapitel 2: Freiheit der Meinungsäußerung und Presse	248
A. Schutzbereich	248
B. Beeinträchtigung	250
C. Rechtfertigung	252
I. Vereinbarkeit mit Art. 10 Abs. 1 EMRK	252
1. Massenüberwachung und Zugriff auf Individualkommunikation	253
2. Datenbezug von fremden Nachrichtendiensten	255
II. Vereinbarkeit mit Art. 19 Abs. 2 IPbpr	256
D. Schutzpflichten	257
Unterkapitel 3: Recht auf wirksame Beschwerde	258
A. Schutzbereich	258
B. Beeinträchtigung	260
C. Rechtfertigung	261
Unterkapitel 4: Schutz des Eigentums	262
A. Schutzbereich	262
B. Beeinträchtigung	263
Kapitel 4: Verfahrensrechtliche Bezüge	266
A. Staatenbeschwerden	266
B. Individualbeschwerden	268
I. Vereinbarkeit mit den Konventionen	269

II. Opfereigenschaft	270
1. EMRK	270
a) Allgemeine Grundsätze	270
b) Ausnahmen bei verdeckter Telekommunikationsüberwachung	271
2. IPbpr	273
a) Allgemeine Grundsätze	273
b) Ausnahmen bei verdeckter Telekommunikationsüberwachung?	274
III. Subsidiarität und Litispendenz	275
1. Subsidiarität	275
2. Litispendenz	276
 Teil 5: Zusammenfassung der Untersuchungsergebnisse	 279
 Literaturverzeichnis	 289
 Journalistische Quellen und amtliche Veröffentlichungen	 299